

CLAIMS

1  
Claim ~~47~~ (previously amended): A method of encrypting an electronic file in an application program running in a suitable environment for operating the program, comprising the steps of:

- a) issuing a change document command to act upon the file;
- b) intercepting the change document command;
- c) acquiring an encryption key value;
- d) encrypting the file using the encryption key value to create an encrypted file;
- e) completing the change document command by performing the change document

command upon the encrypted file instead of the file; and

- 2  
f) invoking an option to initiate a virus scan program;

wherein steps c) and d) further comprise the steps of:

selecting an algorithm to use with the file from one of a plurality of encryption

algorithms;

selecting an encryption key with a key value;

generating a file identifier from the encryption key, an algorithm identifier associated

with the selected algorithm and a data identifier associated with the file;

adding the file identifier to the file; and

using the key value and the selected algorithm to encrypt the file.

Claim ~~48~~ (previously amended): The method as recited in claim ~~47~~, comprising the further step of running a virus scan program on the file before it is encrypted.

Claim <sup>3</sup>~~49~~ (previously amended): The method as recited in claim <sup>1</sup>~~47~~, comprising the further steps of selecting the file from within the contents of a second file that is larger than the file.

Claim <sup>4</sup>~~50~~ (previously amended): The method as recited in claim <sup>3</sup>~~49~~, comprising the further steps of creating a third file from the second file wherein the third file contains the encrypted file and the portion of the second file that does not include the file.

Claim <sup>5</sup>~~51~~ (previously amended): The method as recited in claim <sup>4</sup>~~50~~, wherein the encrypted file is located in a container.

Claim <sup>6</sup>~~52~~ (previously amended): The method as recited in claim <sup>1</sup>~~47~~, wherein the algorithm is selected from the plurality of algorithms according to a pre-selected criteria.

Claim <sup>7</sup>~~53~~ (previously amended): The method as recited in claim <sup>6</sup>~~47~~, wherein the algorithm is selected from the plurality of algorithms according to a pre-selected algorithm.

Claim <sup>8</sup>~~54~~ (previously amended): The method as recited in claim <sup>11</sup>~~47~~, wherein the file identifier is inserted into the file according to a pre-selected criteria.


Claim <sup>9</sup>~~55~~ (previously amended): The method as recited in claim <sup>1</sup>~~47~~, wherein the file identifier is inserted into the file according to a pre-selected algorithm.

Claim <sup>10</sup>~~56~~ (previously amended): The method as recited in claim <sup>1</sup>~~47~~, wherein there are plural encryption key values and at least one encryption key value is associated with the user.

Claim <sup>11</sup>~~57~~ (previously amended): The method as recited in claim <sup>10</sup>~~56~~, comprising the further steps of:

requiring the user to submit to an access authentication step; and  
if the access authentication step does not authenticate the user, then skipping steps c) and d), but if the access authentication step does authenticate the user, then retrieving the encryption key value associated with the encryption key name and the user.

<sup>12</sup>  
Claim 58 (previously amended): A method of decrypting an electronic file that is to be opened in an application program running in a suitable environment for operating the program, comprising the steps of:

- 
- a) issuing an open document command to act upon the file;
  - b) intercepting the open document command;
  - c) retrieving a decryption key value;
  - d) decrypting the file using the decryption key value to create an unencrypted file;

and

e) completing the open document command by performing the open document command upon the unencrypted file instead of the file; and

wherein steps c) and d) further comprise the steps of:

selecting an algorithm to use with the file from one of a plurality of algorithms;

selecting an encryption key with a key value;

inputting a decryption key with a key value;

validating the decryption key value with the key value associated with a file identifier;

using the key value and the selected algorithm to decrypt the file; and

invoking an option to initiate a virus scan program.

~~Claim 59 (previously amended): A method of decrypting an electronic file that is to be opened in an application program running in a suitable environment for operating the program, comprising the steps of:~~

- ~~a) issuing an open document command to act upon the file;~~
- ~~b) intercepting the open document command;~~
- ~~c) retrieving a decryption key value;~~
- ~~d) decrypting the file using the decryption key value to create an unencrypted file;~~

and

~~e) completing the open document command by performing the open document command upon the unencrypted file instead of the file; and~~

~~wherein steps c) and d) further comprise the steps of:~~

~~selecting an algorithm to use with the file from one of a plurality of algorithms;~~

~~inputting a decryption key with a key value;~~

~~validating the decryption key value with the key value associated with a file identifier;~~

~~using the key value and the selected algorithm to decrypt the file; and~~

~~running a virus scan program on the decrypted file.~~

~~60 (previously amended): A method of encrypting and decrypting a file with one of a plurality of algorithms, comprising the steps of:~~

~~selecting an algorithm to use with the file from the plurality of algorithms;~~

~~selecting an encryption key with a key value;~~

generating a file identifier from the encryption key, an algorithm identifier associated with the selected algorithm and a data identifier associated with the file;

adding the file identifier to the file;

using the key value and the selected algorithm to encrypt the file and generate an encrypted file;

uniquely identifying the encrypted file with an encrypted data identifier during encryption;

inputting a decryption key with a decryption key value;

validating the decryption key value with the key value associated with the file identifier;

using the key value and the selected algorithm to decrypt the file; and

testing the encrypted data identifier after decryption by regenerating the encrypted data identifier and ascertaining that they are the same.

15  
61 (previously amended) The method as recited in claim 60<sup>14</sup>, comprising the further step of selecting the file from within the contents of a second file that is larger than the file.

16  
62 (previously amended) The method as recited in claim 61<sup>15</sup>, wherein the encrypted file is placed in a container.

17  
Claim 63 (currently amended): The method as recited in claim 62, comprising the further step of A method of encrypting and decrypting a file with one of a plurality of algorithms, comprising the steps of:

selecting an algorithm to use with the file from the plurality of algorithms

selecting an encryption key with a key value

generating a file identifier from the encryption key, an algorithm identifier associated  
with the selected algorithm and a data identifier associated with the file  
adding the file identifier to the file  
using the key value and the selected algorithm to encrypt the file and generate an  
encrypted file  
uniquely identifying the encrypted file with an encrypted data identifier during encryption  
inputting a decryption key with a decryption key value  
validating the decryption key value with the key value associated with the file identifier  
using the key value and the selected algorithm to decrypt the file  
testing the encrypted data identifier after decryption by regenerating the encrypted data  
identifier and ascertaining that they are the same  
selecting the file from within the contents of a second file that is larger than the file  
creating a third file from the second file wherein the third file contains the encrypted file  
and the portion of the second file that does not include the file  
wherein the encrypted file is placed in a container.

<sup>16</sup>Claim ~~64~~ (previously amended): The method as recited in claim <sup>17</sup>~~63~~, wherein the container is represented in the third file.

<sup>19</sup>Claim ~~65~~ (previously amended): The method as recited in claim <sup>18</sup>~~64~~, wherein the decryption is initiated with whatever method is appropriate to the way the file is represented in the third file.

<sup>20</sup>Claim ~~66~~ (previously amended): The method as recited in claim <sup>18</sup>~~64~~, wherein the second file is recreated from the third file after the file is decrypted.

<sup>21</sup> Claim ~~67~~ (previously amended): The method as recited in claim ~~66~~<sup>20</sup>, comprising the further step of running a virus scan program on the second file after it is recreated.

<sup>1</sup> Claim 68 (previously amended): A method of encrypting and decrypting a file with one of a plurality of algorithms, comprising the steps of:

selecting an algorithm to use with the file from the plurality of algorithms;

selecting an encryption key with a key value;

generating a file identifier from the encryption key, an algorithm identifier associated with the selected algorithm and a data identifier associated with the file;

adding the file identifier to the file;

inputting a decryption key with a decryption key value;

validating the decryption key value with the key value associated with the file identifier;

and

using the key value and the selected algorithm to decrypt the file;

wherein the file is located in a document or image repository.

Claim 69 (previously amended): A method of encrypting and decrypting a file with one of a plurality of algorithms, comprising the steps of:

selecting an algorithm to use with the file from the plurality of algorithms;

selecting an encryption key with a key value;

generating a file identifier from the encryption key, an algorithm identifier associated with the selected algorithm and a data identifier associated with the file;

adding the file identifier to the file;

8/22

using the key value and the selected algorithm to encrypt the file and generate an encrypted file;  
sending the encrypted file from a first person to a second person over the Internet in an e-mail message;  
inputting a decryption key with a decryption key value;  
validating the decryption key value with the key value associated with the file identifier;  
and  
using the key value and the selected algorithm to decrypt the file.

Claim 70 (previously amended): The method as recited in claim 69, wherein the first person is the same as the second person.

Claim 71 (previously amended): A method of encrypting and decrypting a file with one of a plurality of algorithms, comprising the steps of:

selecting an algorithm to use with the file from the plurality of algorithms;  
selecting an encryption key with a key value;  
generating a file identifier from the encryption key, an algorithm identifier associated with the selected algorithm and a data identifier associated with the file;  
adding the file identifier to the file;  
using the key value and the selected algorithm to encrypt the file and generate an encrypted file;  
inputting a decryption key with a decryption key value;



validating the decryption key value with the key value associated with the file identifier;  
and  
using the key value and the selected algorithm to decrypt the file;  
wherein a portion of the file identifier is encrypted before it is inserted into the file.

Claim 72 (previously amended): The method as recited in claim 71, comprising the further step of decrypting a portion of the file identifier before the decryption key value is validated.

Claim 73 (previously amended): The method as recited in claim 72, wherein all of the file identifier is encrypted before the decryption key value is validated.

Claim 74 (previously amended): A method of encrypting and decrypting a file with one of a plurality of algorithms, comprising the steps of:

selecting an algorithm to use with the file from the plurality of algorithms;  
selecting an encryption key with a key value;  
generating a file identifier from the encryption key, an algorithm identifier associated with the selected algorithm and a data identifier associated with the file;  
adding the file identifier to the file;  
using the key value and the selected algorithm to encrypt the file and generate an encrypted file;  
inputting a decryption key with a decryption key value;  
validating the decryption key value with the key value associated with the file identifier;  
using the key value and the selected algorithm to decrypt the file;  
invoking an option to initiate a virus scan program.

10/22

~~Claim 75 (previously amended): A method of encrypting and decrypting a file with one of a plurality of algorithms, comprising the steps of:~~

~~selecting an algorithm to use with the file from the plurality of algorithms;~~

~~selecting an encryption key with a key value;~~

~~generating a file identifier from the encryption key, an algorithm identifier associated with the selected algorithm and a data identifier associated with the file;~~

~~adding the file identifier to the file;~~

~~running a virus scan program on the file before it is encrypted;~~

~~using the key value and the selected algorithm to encrypt the file and generate an encrypted file;~~

~~inputting a decryption key with a decryption key value;~~

~~validating the decryption key value with the key value associated with the file identifier;~~

~~and~~

~~using the key value and the algorithm to decrypt the file;~~

~~wherein a portion of the file identifier is encrypted before it is inserted into the file.~~

~~Claim 76 (previously amended): A method of encrypting a file with one of a plurality of algorithms, comprising the steps of:~~

~~selecting an algorithm to use with the file from the plurality of algorithms;~~

~~selecting an encryption key with a key value;~~

~~generating a file identifier from the encryption key, an algorithm identifier associated with the selected algorithm and a data identifier associated with the file;~~

adding the file identifier to the file; and

uniquely identifying the encrypted file with an encrypted file header.

1  
D  
/ Claim 77 (previously amended): A method of decrypting an encrypted file with one of a plurality of algorithms, comprising the steps of:

selecting an algorithm to use with the encrypted file from the plurality of algorithms;

inputting an decryption key with a decryption key value;

validating the decryption key value with the key value associated with a file identifier that was added to a file during an encryption process that created the encrypted file;

using the key value and the selected algorithm to decrypt the file;

testing the encrypted data identifier that is used to uniquely identify the encrypted file during the encryption process by regenerating the encrypted data identifier and ascertaining that they are the same.

/ Claim 78 (previously added): A method of encrypting and decrypting a file with one of a plurality of algorithms, the method comprising the steps of

selecting an algorithm to use with the file from the plurality of algorithms

selecting an encryption key with a key value

generating a file identifier from the encryption key, an algorithm identifier associated with the selected algorithm and a data identifier associated with the file

adding the file identifier to the file

using the key value and the selected algorithm to encrypt the file and generate an encrypted file

12/22

✓ sending the encrypted file from a first person to a second person in an e-mail message.

67  
✓ Claim 79 (previously added): A method of encrypting and decrypting a file with one of a plurality of algorithms, the method comprising the steps of:

receiving an encrypted file from a first person by a second person in an e-mail message

extracting a file identifier from the file

inputting a decryption key with a decryption key value

validating the decryption key value with a key value associated with the file identifier

using the key value and the selected algorithm to decrypt the file.

✓ 2  
13  
✓ 80. (New claim) The method as recited in claim 78, comprising the further step of running a virus scan program on the decrypted file. ~